



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
NETWORK ENTERPRISE TECHNOLOGY COMMAND
REGIONAL CHIEF INFORMATION OFFICE, REPUBLIC OF KOREA REGION
UNIT # 15271
APO AP 96205-5271

NETC-SKC-IO

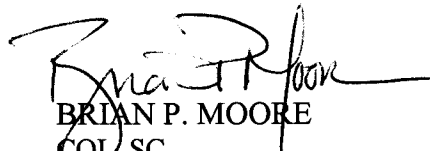
29 DEC 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Korea LandWarNet (UNCLAS) Acceptable Use Policy (AUP)

1. The provisions of AR 25-2, Information Assurance, 14 Nov 03, Paragraph 4-5, direct the minimum information assurance requirements for all Army systems and networks. All new users will be required to read and sign this AUP prior to accessing UNCLAS Network Resources on the LandWarNet. This AUP coupled with initial user security training will improve user security awareness across the peninsula and reduce the insider threat (intentional or unintentional) to our LandWarNet (UNCLAS) systems.
2. This Korea LandWarNet (UNCLAS) AUP supercedes AUP, Regional Chief Information Office, Republic of Korea Region, 20 August 2004, Subject: Acceptable Use Policy and is effective immediately.
3. POC for this action is GS12 Rodney Wagar, DSN 723-2373, rodney.wagar@us.army.mil.

Encl


BRIAN P. MOORE
COL, SC
Regional Chief Information Officer

DISTRIBUTION:
Electronic Media Only (EMO)

For Official Use Only

Korea LandWarNet (UNCLAS) Acceptable Use Policy
1 December 2006

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the Sensitive Information NIPRNet from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.

2. **Access.** Access to the LandWarNet is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation", AR 25-2, "Information Assurance" or as further limited by this policy.

3. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Unclassified information processing.** Your assigned government system on the LandWarNet is an unclassified information system for your organization.

a. Your government system provides unclassified communication to your organization, the military services, external DOD elements, and other United States Government organizations. Primarily this is done via electronic mail and through the World Wide Web. Your government system is approved to process Sensitive Information.

b. Your government system and the Korea LandWarNet, as viewed by your organization, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the LandWarNet, and Internet. Data sent in e-mail and attachments need to be reviewed and verified (encrypt if necessary) by the user before being sent over the unclassified sensitive network.

5. **Minimum security rules, requirements, and unacceptable use.** As a government system user, the following minimum security rules and requirements apply. I understand that monitoring of my assigned government system will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities include unacceptable uses of a government information system (IS):

(Initials)

_____ a. Personnel are not permitted access to any government system unless authorized, trained, and only after reading and completing this Acceptable Use Policy. I have completed the user security awareness training module. I will participate in all training programs as required both before receiving system access and when refresher training is required.

_____ b. I will generate and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of upper and lowercase letters, 2 numbers, and 2 special characters. I am the only authorized user of my account. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

Korea LandWarNet (UNCLAS) Acceptable Use Policy

1 December 2006

_____ c. I will use only authorized government hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software. I will not disable or remove security or protective software or mechanisms and their associated logs. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized. I will not introduce executable code (such as, but not limited to .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code. I will not add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications, spyware, chat programs, etc). I will not attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring. (i.e. change proxy settings in web browser)

_____ d. I will use Theater Network Operations Support Center (TNOSC) located at Camp Walker Taegu-provided virus-checking software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive, or any other removable and/or portable storage devices. If TNOSC-provided software is not available, I will utilize the software available on the Army Computer Emergency Response Team (ACERT) website.

_____ e. I will safeguard and follow guidance on protection strategy for Data at Rest (DAR) devices. These devices include, but are not limited to, laptops, portable notebooks, tables-PC's, thumb drives, external media, and similar systems; referred to as Mobile Computing Device (MCDs); which are highly susceptible to theft and loss. These devices are identified as high-risk when authorized for use in remote computing scenarios. All users must ensure that our sensitive information is protected and defended against unauthorized release. Encrypt all sensitive data on DAR devices.

_____ f. I will safeguard (and mark with the appropriate classification level, if required) all information created, copied, stored, or disseminated from the information system and will not disseminate it to anyone without a specific need to know. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need-to-know. I will not release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

_____ g. I will not utilize Army or DOD provided information systems for commercial, financial gain or illegal activities. I will not use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct. I will not intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.). I will not misuse government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of

Korea LandWarNet (UNCLAS) Acceptable Use Policy
1 December 2006

copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

_____ h. I will address any questions regarding policy, responsibilities, and duties to my unit IMO and/or IASO. Maintenance will be performed by the Systems Administrator, Information Management Officer, or servicing DOIM only.

_____ i. I will use screen locks when leaving my system for short periods of time and log off the system when departing the area for extended periods. I will perform a restart on my government system each work day to ensure that updates are applied and to improve performance.

_____ j. I will immediately report any suspicious output, files, shortcuts, or system problems to my unit IMO and/or IASO. I will report all known or suspected security incidents, spam, chain letters, or violations of this acceptable use policy and/or AR 25-2 to the IASO, IMO, and DOIM.

_____ k. I understand that each information system is the property of the government and is provided to me for official and authorized uses. I further understand that each information system is subject to monitoring for security purposes and to ensure use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the information system and may have only a limited expectation of privacy in personal data on the information system. I realize that I should not store data on the information system that I do not want others to see.

6. Penalties. I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or other administrative and criminal statutes. These violations are covered under paragraph 1-1j. of AR 25-2.

7. Acknowledgement. I have read the above requirements regarding use of my assigned government system on the Korea LandWarNet. I understand my responsibilities regarding my government system and the information contained in them.

Unit/Division/Branch

Date

Last Name, First, MI

Rank/Grade

Signature

Phone Number

Korea LandWarNet (UNCLAS) Acceptable Use Policy
Korea LandWarNet (UNCLAS) 사용 수칙
1 December 2006

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the Sensitive Information NIPRNet from unauthorized or inadvertent modification, disclosure, destruction, denial or service, and use.

약속. 한국 국가기밀 정보망인 NIPRNet 사용시, 본사용자는 허가를 받지 않은 상태로 정보에 접근하거나, 수정, 유출, 파손, 부정 사용을 하지 않겠습니다.

2. Access. Access to the LandWarNet is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation", AR 25-2, "Information Assurance" or as further limited by this policy.

사용. LandWarNet 사용은 DOD 5500.7-R, "Joint Ethics Regulation", AR 25-2, "Information Assurance"와, 본 사용수칙에 명시된 바 대로, 공적으로 인가된 상태에서만 가능합니다.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

취소. 미육군 정보에 대한 접근은 언제든지 취소될 수 있으며, (당국은 꾸준한 모니터링과 보안 유지를 수행할 것입니다) 보안유지를 위해 모든 시스템은 모니터링되고 테스트될 수 있음을 인지합니다.)

4. Unclassified information processing. Your assigned government system on the LandWarNet is an unclassified information system for your organization.

일반 정보 처리. 개인에게 할당된 LandWarNet 의 정부 시스템은 개인이 소속되어 있는 조직을 위한 일반 정보 시스템입니다.

a. Your government system provides unclassified communication to your organization, the military services, external DOD elements, and other United States Government organizations. Primarily this is done via electronic mail and through the World Wide Web. Your government system is approved to process Sensitive Information.

모든 정부 시스템은 해당 부대, 군 기관, 미 국방성과 연계된 외부 기관을 비롯해 미 정부 기관에 일반적인 정보를 제공하는데, 이것은 주로 World Wide Web)과 e-mail 로 이루어집니다. 이 정부 시스템들은 국가 안보에 중요한 정보를 처리할 수 있도록 승인되어 있습니다.

b. Your government system and the Korea LandWarNet, as viewed by your organization, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the LandWarNet, and Internet. Data sent in e-mail and attachments need to be reviewed and verified (encrypt if necessary) by the user before being sent over the unclassified sensitive network.

미국 정부 시스템과 Korea LandWarNet 은 국내에 있는 모든 미군관련 기관에게는 같은 의미를 갖습니다. e-mail 과 첨부 파일들은 LandWarNet 와 인터넷을 통해 전송될 때 누군가가 훔쳐볼 위험이 있습니다. e-mail 과 첨부 파일에 포함된 내용들은 일반 정보망을 통해 보내지기 전에 충분히 검토되고, 필요 시 암호화가 되어야 합니다.

Korea LandWarNet (UNCLAS) Acceptable Use Policy

Korea LandWarNet (UNCLAS) 사용 수칙

1 December 2006

5. Minimum security rules, requirements, and unacceptable use. As a government system user, the following minimum security rules and requirements apply. I understand that monitoring of my assigned government system will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities include unacceptable uses of a government information system (IS):

최소한의 보안 규정과 요건, 사용금지. 정부 시스템 사용자는 다음과 같은 보안 규정과 요건을 지켜야 합니다. “나는 나에게 할당된 시스템에 다양한 목적의 모니터링이 이루어질 수 있다는 것을 이해합니다. 또한 모니터링 중에 포착한 정보가 행정처벌과 범죄수사의 결과를 낼 수도 있음을 인지합니다.”. 본 사용자는 미정부 정보 시스템을 이용하여 다음과 같은 행동들을 할 수 없음을 인지합니다..

(Initials)

_____ a. Personnel are not permitted access to any government system unless authorized, trained, and only after reading and completing this Acceptable Use Policy. I have completed the user security awareness training module. I will participate in all training programs as required both before receiving system access and when refresher training is required.

본인은 본 사용 수칙에 대한 충분한 이해와 당국의 허가, 훈련 없이 정부 시스템을 사용할 수 없습니다. 또한 본인은 사용자 비밀 보안 유지 준수 훈련을 받았습니다. 또, 시스템 사용 권한을 얻기 전, 또 재훈련이 필요하다고 판단되면 훈련 프로그램에 참가하겠습니다

_____ b. I will generate and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of upper and lowercase letters, 2 numbers, and 2 special characters. I am the only authorized user of my account. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

본인은 암호와 비밀번호를 만들어 철저히 보안을 유지하겠습니다. 최소한 영문 대문자 소문자 각각 2 개, 숫자 2 개 그리고 특수문자 2 개를 섞어서 10 자 이상의 암호를 만들겠습니다. 본인은 본인이 사용하는 계정에 유일하게 접속할 수 있는 사람으로, 개인 계정 및 암호를 타인에게 유출하지 않을 것이며, 어느 누구의 원거리 접근도 막겠습니다.

_____ c. I will use only authorized government hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software. I will not disable or remove security or protective software or mechanisms and their associated logs. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized. I will not introduce executable code (such as, but not limited to .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code. I will not add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications, spyware, chat programs, etc). I will not attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring. (i.e. change proxy settings in web browser)

본인은 인가된 정부 하드웨어와 소프트웨어만을 사용하겠습니다. 또한, 개인 소유의 하드웨어, 소프트웨어, 셰어웨어 또는 공공 소프트웨어를 설치하거나 이용하지

Korea LandWarNet (UNCLAS) Acceptable Use Policy

Korea LandWarNet (UNCLAS) 사용 수칙

1 December 2006

않겠습니다. 보안 보호 소프트웨어 또는 메커니즘 그리고 그와 관련된 기록들(logs)을 파손시키거나 제거하지 않습니다. 운영 체제, 프로그램들을 허락 없이 수정, 변환, 설정 또는 사용하지 않습니다. 실행코드(.exe, .com, .vbs 또는 .bat 등의 파일들)를 허락 없이 들여오지 않고 유해한 코드를 쓰지 않습니다. 사용자가 변경할 수 있거나 공중되지 않은 소프트웨어 (메신저, P2P, 스파이웨어, 채팅)는 사용하지 않습니다. 보안 메커니즘을 남용, 시험, 방해하거나 간과하지 않습니다. (예를 들면, 웹 브라우저에서 프락시 설정 변경 등). 또한, 네트워크 망 모니터링, 키보드 기록을 하지 않습니다.

_____ d. I will use Theater Network Operations Support Center (TNOSC) located at Camp Walker Taegu-provided virus-checking software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive, or any other removable and/or portable storage devices. If TNOSC-provided software is not available, I will utilize the software available on the Army Computer Emergency Response Team (ACERT) website.

본인은, 업로드하기 전이나, 다른 시스템, 디스켓, 첨부파일, CD, USB 드라이브, 포터블 저장 장치를 사용할 때, 대구 캠프 워커에 위치한 Theater Network Operation Support Center (TNOSC)에서 제공하는 바이러스 검색 프로그램 및 검색 과정을 반드시 사용하겠습니다. 만약 TNOSC 의 제공 소프트웨어 사용이 불가능하다면, Army Computer Emergency Response Team(ACERT) 웹사이트가 제공하는 유틸리티를 사용하겠습니다.

_____ e. I will safeguard and follow guidance on protection strategy for Data at Rest (DAR) devices. These devices include, but are not limited to, laptops, portable notebooks, tables-PC's, thumb drives, external media, and similar systems; referred to as Mobile Computing Device (MCDs); which are highly susceptible to theft and loss. These devices are identified as high-risk when authorized for use in remote computing scenarios. All users must ensure that our sensitive information is protected and defended against unauthorized release. Encrypt all sensitive data on DAR devices.

본인은 Data At Rest (DAR) 장비에 관한 보호규칙을 따르겠습니다. 이 장비들은 노트북, 테블릿 PC, 보조기억매체에 한정되지 않고 쉽게 도난되거나 분실될 수 있는 모든 휴대용 저장매체 (MCDs)를 포함합니다. 이 장비들은 허가된 remote 컴퓨터 사용환경에서도 위험성이 많은 장비로 분류되어 있습니다. 모든 사용자들은 기밀이 보호되어 있고 허가되지 않은 유출로부터 보호하여야 한다. DAR 장비의 모든 기밀들은 암호화 되어야 한다.

_____ f. I will safeguard (and mark with the appropriate classification level, if required) all information created, copied, stored, or disseminated from the information system and will not disseminate it to anyone without a specific need to know. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need-to-know. I will not release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

Korea LandWarNet (UNCLAS) Acceptable Use Policy

Korea LandWarNet (UNCLAS) 사용 수칙

1 December 2006

본인은 미 정보망으로부터 생성되어, 복사, 저장되고 유포된 모든 정보를 보호하겠습니다. (필요시엔 적절한 기밀등급을 표시하겠습니다.) 또한, 필요 없이 아무에게나 정보를 유포하지 않겠습니다. 또, 본인의 비밀 인가 등급을 벗어나, 다뤄서는 안될 정보를 취득하려 하지 않겠으며, 비밀 인가 등급이 허용하는 범위 내에서 본인이 업무상 알아야 할 정보만을 다루겠습니다. 또 본인은, 정보 소유자, AR 380-5 에 명시되어 있는 OCA(Original Classification Authority), 각 개인의 명령 계통상의 책임자, FOIA(Freedom of Information Act), 공보실 또는 보안 담당자의 동의 없이 데이터를 누설, 유출, 수정하지 않겠습니다.

_____ g. I will not utilize Army or DOD provided information systems for commercial, financial gain or illegal activities. I will not use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct. I will not intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.). I will not misuse government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

본인은, 미 육군 또는 미 국방부에서 제공하는 정보 시스템을 상업적, 금전적 목적을 위해서나 불법 활동을 하는 데 사용하지 않겠습니다. 또한, 정보 시스템을 사용할 때, 공식 업무나 준비태세에 절대 방해하지 않겠습니다. 또, 미군에 해가 되거나 윤리적 기준에 어긋나는 행동을 하지 않겠습니다. 또, 외설적, 위협적, 비방적, 정치적 활동과 업무에서 벗어난 활동(즉, spam)을 하지 않겠으며, 이에 상응한 커뮤니케이션 (LE/CI 수사관, 변호사 등이 공식적 업무를 할 때만 이 규정에 저촉되지 않는다.)도 하지 않겠습니다. 또한 온라인 도박이나 공공 서비스에 위배되는 행동도 하지 않겠습니다.

_____ h. I will address any questions regarding policy, responsibilities, and duties to my unit IMO and/or IASO. Maintenance will be performed by the Systems Administrator, Information Management Officer, or servicing DOIM only.

본인은, 규정, 책임, 의무에 관해 의문 사항이 있을 때, 부대 IMO 나 IASO 에게 보고하겠습니다. 정보망 관리는 시스템 관리자, IMO, DOIM 만이 할 수 있습니다.

_____ i. I will use screen locks when leaving my system for short periods of time and log off the system when departing the area for extended periods. I will perform a restart on my government system each work day to ensure that updates are applied and to improve performance.

본인은 화면 보호기 암호를 사용하고, 자리를 비울 상황에선 로그오프를 하겠습니다. 프로그램 자동 업데이트와 향상된 업무를 위해 매일 시스템을 켜고 다시 켜겠습니다.

_____ j. I will immediately report any suspicious output, files, shortcuts, or system problems to my unit IMO and/or IASO. I will report all known or suspected security incidents,

Korea LandWarNet (UNCLAS) Acceptable Use Policy

Korea LandWarNet (UNCLAS) 사용 수칙

1 December 2006

spam, chain letters, or violations of this acceptable use policy and/or AR 25-2 to the IASO, IMO, and DOIM.

본인은 의심되는 출력, 파일, 단축 아이콘이나 시스템 문제를 부대 IMO 나 IASO 에게 즉시 보고하겠으며, 모든 보안 사고, spam, 연쇄 메일(chain letter), 본 사용 수칙이나 AR 25-2 에 위배되는 행위를 IASO, IMO, DOIM 에게 보고하겠습니다.

____ k. I understand that each information system is the property of the government and is provided to me for official and authorized uses. I further understand that each information system is subject to monitoring for security purposes and to ensure use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the information system and may have only a limited expectation of privacy in personal data on the information system. I realize that I should not store data on the information system that I do not want others to see.

모든 정보 시스템이 정부의 재산이며, 본인은 업무상 승인된 목적으로만 이를 사용해야 함을 알고 있습니다. 또한, 본인은 당국이 정보 시스템이 승인된 용도로만 사용되는지 늘 주시하고 있다는 것을 알고 있습니다. 또, 정보 시스템에 저장된 업무적인 데이터에선 사용자의 사생활 보호를 기대할 수 없고, 개인적인 데이터도 제한적으로만 보호됨을 알고 있습니다. 또한, 타인에게 공개하고 싶지 않은 사생활을 정보 시스템에 저장해서는 안 된다는 것을 알고 있습니다.

6. Penalties. I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or other administrative and criminal statutes. These violations are covered under paragraph 1-1j. of AR 25-2.

처벌. 본인이, 이 사용 수칙을 어길 시엔, UCMJ Article 92 와 이와 관련된 행정적, 범죄적 규정에 의해 처벌 받을 수 있음을 알고 있습니다. 이와 같은 규정 침해는 AR 25-2 의 1-1j 에 언급되어 있습니다.

7. Acknowledgement. I have read the above requirements regarding use of my assigned government system on the Korea LandWarNet. I understand my responsibilities regarding my government system and the information contained in them.

본인은 위에 언급된 LandWarNet 시스템에 대한 사용 수칙을 읽었으며, 정부 시스템과 거기에 들어있는 정보에 대한 본인 자신의 책임을 충분히 이해했습니다.

Unit/Division/Branch

Date

Last Name, First, MI

Rank/Grade

Signature

Phone Number